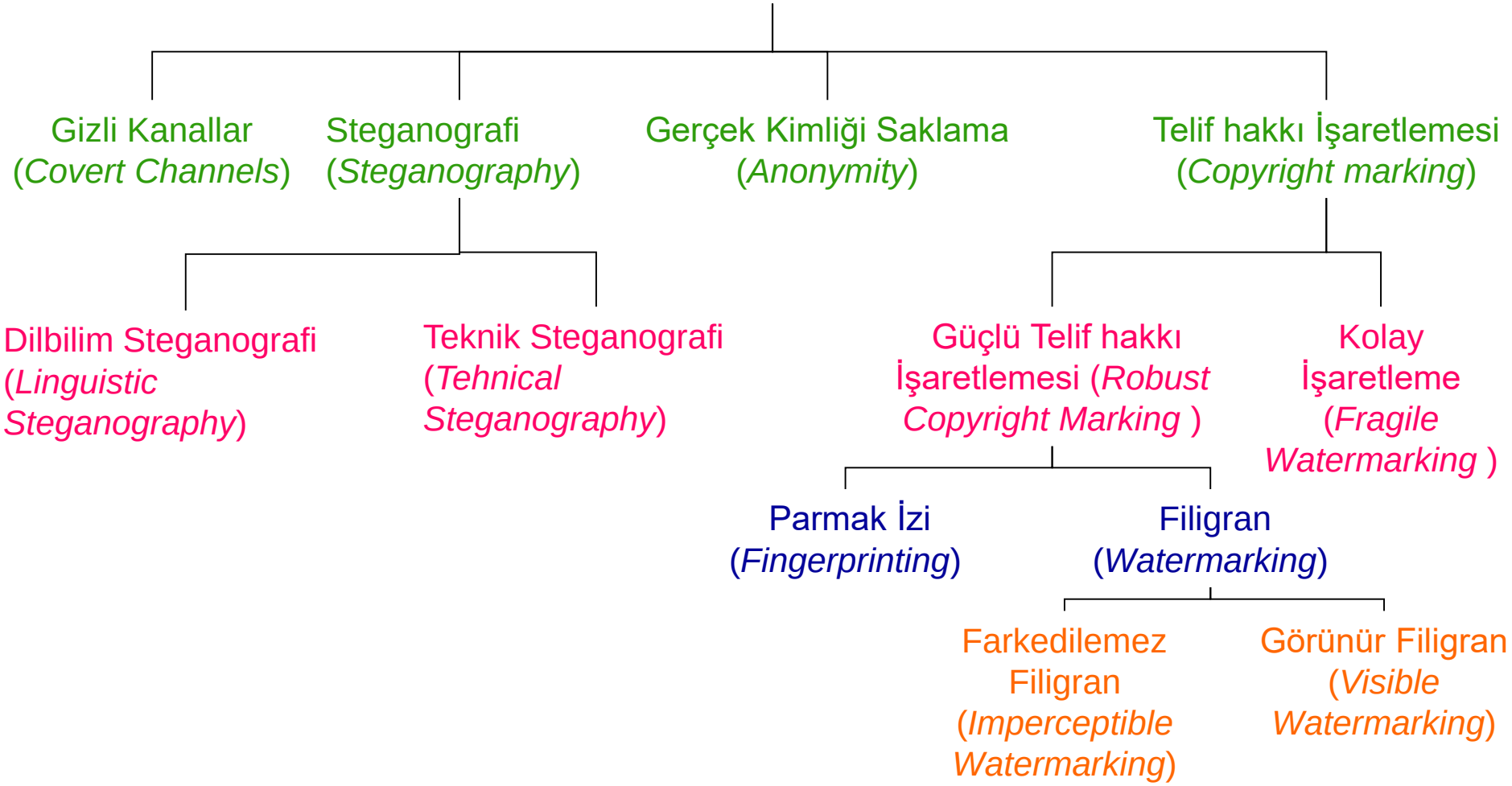
Konu Başlıkları

- Metin Steganografi
- Resim Steganografi
- Ses Steganografi

Bilgi Gizleme

- Bilgi gizleme bir mesajın yada bilginin, herhangi bir masum görünüşlü ortam içine saklanarak bir diğer kişiye iletilmesidir.
- Bilgi gizleme bilgisayar ortamındaki encapsulation işlemine benzer bir durumdur.
  - Encapsulation (Kapsülleme)
    - Bir modülün yaptığı işlemlerin bir kısmını, bu işlemleri nasıl gerçekleştirdiği bilgisini dışarıdan bilinçli olarak saklamaktır.
    - Encapsulation'ın asıl amacı içeriği saklamak değil kontrolsüz ve gereksiz erişimi engellemek, dış öğeleri, içeriğe standart, önceden tanımlı arayüzler aracılığıyla ulaşıma zorlamaktır.

Bilgi Gizleme



Gizli Kanallar (Covert Channels)

İki kişi arasında gizli bilgilerin eldeğiştirmesi için iletişimi sağlayan kanaldır. Gizli kanal kurulması iki kişinin karşılıklı anlaşmasını gerektirmektedir.

Gizli Kanalların amaçları:

- İletişimimizdeki veriyi saklamaya çalışmak
- İletişiminin amacını saklamak

Gizli Kanallar (Covert Channels)

Böylece;

- Gerçek veri transferi, dikkatsiz gözlere zararsız ve kanuna uygunmuş gibi gözükecektir.
- Veriyi karıştırmak için ayrı bir şifreleme yapılmasına gerek kalmayacaktır.

Gizli Kanallar (Covert Channels)

- Gizli Kanallar çeşitli alanlarda kullanılmaktadır. Bunlar;
  - Dosya tabanlı steganografi
    - Görüntü, ses ve text dosyaları
  - Ağ paket steganografisi
    - Veriler IP paketleri içine gizlenmektedir.
  - Protokol Kapsüllenmesi
    - SSL (Secure Sockets Layer) üstünde TCP paketleri içerisine
    - SSH (Secure Shell) üstünde TCP paketleri içerisine

Gerçek Kimliği Saklama (Anonymity)

- Veri gönderimi sırasında gerçek kimliği saklayarak bilginin bilinmeyen yada anlaşılamayan biri üzerinden gidiyor olduğunu izlenimi verilerek te bilgi zarar görmeden gönderilebilmektedir.
- Fakat ağlar üzerinde bilinmeyen kullanıcı olayı ağ yöneticilerinin daha fazla dikkatini çekmekte ve bilgi güvenliği tehlikeye girmektedir.
- Bu yüzden sadece çok gerektiği durumlarda kullanılması uygundur.

Steganografi (Steganography)

- Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir.
- Ses, sayısal resim, video görüntüleri üzerine veri saklanabilir.
- Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine başka bir görüntüyü gizlemekte olasıdır.

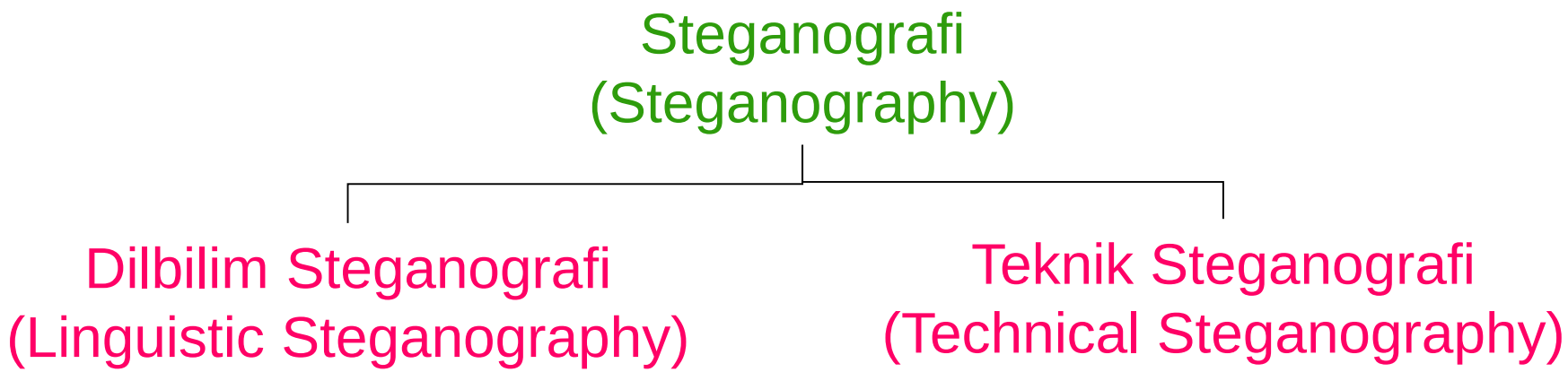
Steganografi

- Bu yaklaşımda içine bilgi gizlenen ortam cover-data (örtü verisi), ve oluşan ortama da stego-text veya stego-object denilmektedir.

- Bir stego-key (stego-anahtarı), bilginin saklaması işlemini kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak için kullanılmaktadır.

Steganografi

Steganografi kendi içinde iki kısma ayrılmaktadır.



Dilbilim Steganografi (Linguistic Steganography)

- Dilbilim steganografi, taşıyıcı verinin text olduğu steganografi koludur.
- Burada veriyi gizlemek için text üzerinde değişiklikler yapılmaktadır.
- Bu değişiklikler şu şekilde yapılabilir.değişiklik yapmanın çeşitli yolları vardır.
- Bunlardan bazıları;
  - grafik kullanılarak yapılabilir
  - text'in yapısı değiştirilerek yapılabilir
  - yada amacı sadece veriyi saklamak olan yeni bir text yaratılabilir

Linguistic Steganography

Dilbilim Steganografi'de kullanılan yöntemler şunlardır:

- Açık kodlar
  - Gizli mesaj, açıkça okunabilir fakat zararsız bir mesaj haline gelir.
  - Bu işlem; maskeleme, boş şifreler ve ızgaralama ile yapılmaktadır.
- Şemagramlar
  - Gizli mesaj, açık metinin ufak fakat gizli bir detayının içine gizlenmektedir.
  - Bunun için grafiksel değişiklikler yapılmaktadır.
  - Kullanılan yöntemler; farklı yazı tipleri kullanmak, eski daktilo yazılarını kullanmak, resimler içinde boşluklar kullanmak vb.

Teknik Steganografi (Technical Steganography)

Teknik Steganografi bir çok konuyu içine almaktadır.

- Bunları bazı başlıklar altında toplayabiliriz;
  - Görünmez mürekkep: Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemidir.
  - Gizli yerler: Kimsenin göremeyeceği gizli yerlere saklama (bavul, kasa vb.)
  - Microdot'lar: Bilgiyi noktalar halinde sayfaya gizleme
  - Bilgisayar tabanlı yöntemler: Text, ses, görüntü, resim dosyalarını kullanarak veri gizleme yöntemleridir.

Steganografinin Kullanım Alanları

- Metin Steganografi (Text Steganography)
- Görüntü Steganografi (Image Steganography)
- Ses Steganografi (Audio Steganography)

Metin Steganografi

- Metin Steganografi taşıyıcı ortamın text olduğu Steganografi alanıdır.
- Metin steganografi genelde uygulanması zor bir veri gizleme şeklidir.
- Metin Steganografi'de saklanacak veri miktarı azdır.
- Bunun nedeni taşıyıcı text'in içindeki gereksiz alanların ve boşlukların miktarının az olmasıdır.
- Metin tabanlı gizleme yöntemlerinin hepsi, gizli mesajı geri çözebilmek için ya orijinal metne, yada orijinal metnin biçimlendirme bilgisine ihtiyaç duyar.

Metin Steganografi

Metin Steganografi veri saklanacak yerlerin özelliklerine göre aşağıdaki yöntemleri kullanır.

1. Açık Alan Yöntemleri (Open Space Methods)
2. Yazımsal Yöntemler
3. Anlamsal Yöntemler

1- Açık Alan Yöntemleri (Open Space Methods)

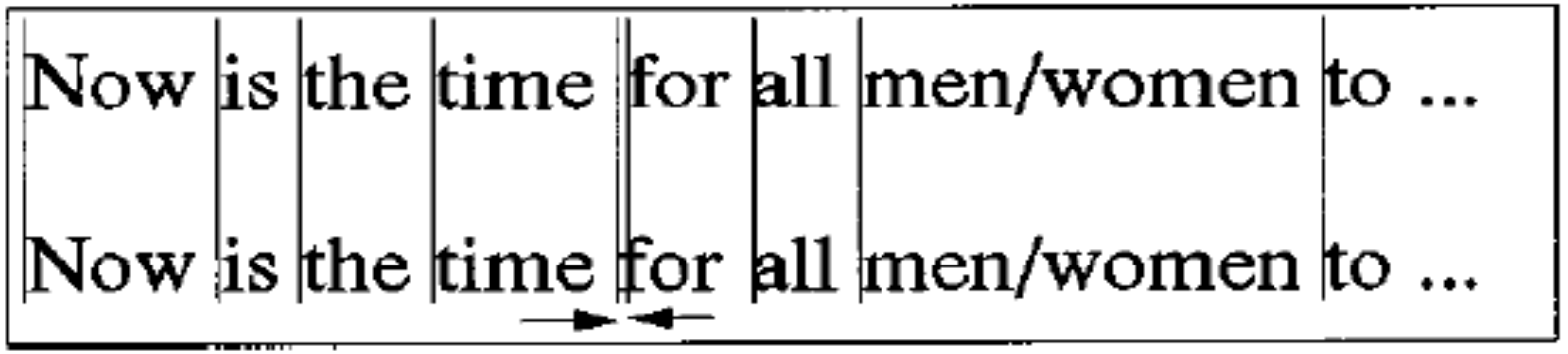
- Bu yöntemler, anormal gözükmeyen iki kelime arasında extra boşluklar, satır sonu boşlukları ile çalışmaktadır.
- Bununla birlikte Açık Alan Yöntemleri'nin ASCII kodları ile kullanılması daha uygundur.

Açık Alan Yöntemleri

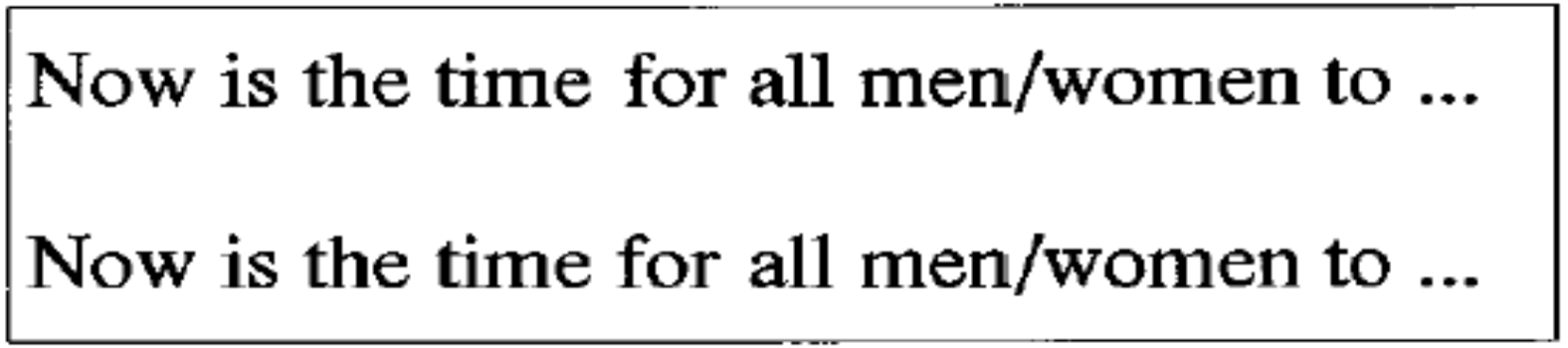
- Açık alan yöntemleri de kendi içerisinde 5 farklı uygulama tipine sahiptir.
  - Cümle içi boşluk bırakma
  - Satır kaydırma
  - Satır sonu boşluk bırakma
  - Sağ hizalama
  - Gelecek kodlaması

a) Cümle İçi Boşluk Bırakma

- Cümle içi boşluk bırakma yöntemi;
  - İngilizce dil yapısında, bir noktadan sonra tek bir boşluk bırakarak “0”ı saklar.
  - Çift boşluk eklemek ise “1”i saklar.
  - Bu işlem işe yarar, ancak çok küçük bir veriyi saklamak için çok büyük veriye ihtiyaç duyar.
  - Bununla birlikte bir çok kelime işleme programı da çift boşlukları otomatik olarak temizler.



(a)



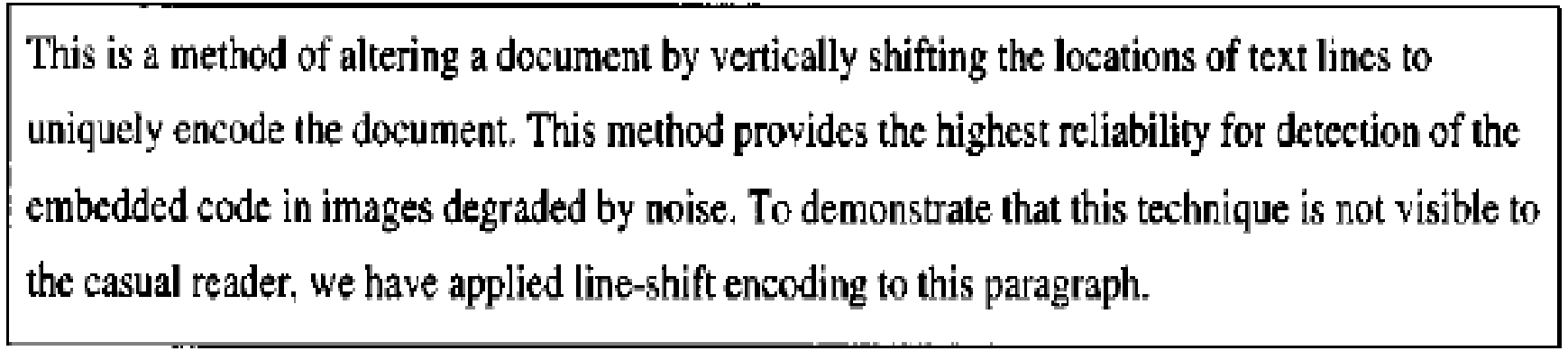
(b)

(a) Üst satır'da "for" kelimesinden önce bir boşluk eklenmektedir, alt satırda for ile all arasında daha fazla boşluk vardır.

(b) Dikey çizgiler olmadan text'in nasıl gözüktüğü

b) Satır Kaydırma Kodlaması

- Bu yöntemde text satırları düşey olarak kaydırılarak gömülecek mesajın kodlanması sağlanır.
- Gömülmüş kelime yine text dosyası yada bitmap dosya olarak açılabilir.


This is a method of altering a document by vertically shifting the locations of text lines to uniquely encode the document. This method provides the highest reliability for detection of the embedded code in images degraded by noise. To demonstrate that this technique is not visible to the casual reader, we have applied line-shift encoding to this paragraph.

Burada ikinci satır 1/300 inch yukarıya kaydırılmıştır.

c) Satır Sonu Boşluk Bırakma

- Satır sonu boşluğu yöntemi, her satırın sonundaki boşluktan faydalanır.
- Veri, tüm satır sonlarında daha önceden belirlenen sayıda boşluklar bırakarak gizlenir.
- Örneğin, iki boşluk bir bit, dört boşluk iki bit, sekiz boşluk dört bit vb. gizler.
- Bu yöntem, iç boşluk metodundan daha iyi çalışır çünkü satır sonundaki boşluk sayısı arttırılarak daha fazla veri gizlenebilir.

d) Sağ Hizalama

- Metinlerin sağa hizalanması da metin dosyalarında veri saklanmasında kullanılabilir.
- Kelimeler arasındaki boşluklar hesaplanıp kontrol edilerek, masum metin dosyalarına veri gizlenebilir.
- Kelimeler arasındaki tek boşluk “0”ı, çift boşluk “1”i temsil eder.

Sağ Hizalama

- Ancak bu yöntem, normal bir boşluk ile gizlenmiş bir boşluk arasındaki farkı anlamak imkansız olduğu için çözme işlemini zorlaştırır.
- Bu amaçla, Manchester kodlamasını temel olan başka bir teknik kullanılır.
- “01” “1” olarak, “10” “0” olarak yorumlanır. Bununla birlikte “00” ve “11” ise null boşluk bitlerini gösterir.

e) Gelecek Kodlaması

- Bu yöntemde, b, d, T gibi harflerin yatay/düşey uzunlukları gibi bazı metin özelliklerini değiştirerek, biçimlendirilmiş metin içine gizli mesajları saklamayla ilgilenir.
- Bu yöntem, her biçimlenmiş metnin, gizli mesaj saklamak için kullanılabilecek çok sayıda özelliği olmasından dolayı, uzak ara durdurulması en zor yöntemdir.

(a)

(b)

(c)

(a) Herhangi bir kodlama yapılmamış orijinal metin.

(b) Sadece seçilen karakterler üzerinde yapılmış gelecek kodlaması.

(c) Gelecek kodlamasının abartılmış gösterimi

2- Yazımsal Yöntemler (Syntactic Methods)

- Bu yöntem, dökümanı kodlamak için noktalama işaretlerini kullanır.
- Örneğin aşağıdaki iki cümle de ilk bakışta aynıymış gibi gözükmektedir, fakat dikkatlice bakıldığında ilk cümlenin fazladan bir ‘,’ işareti içerdiği görülür.
- Bu yapıların biri “1”, diğeride “0” olarak belirlenir ve kodlama işlemi bu şekilde yapılır.
  - “bread, butter, and milk”
  - “bread, butter and milk”

3- Anlamsal Yöntemler (Semantic Methods)

- Bu yöntem W. Bender tarafından ortaya atılmıştır.
- Bu yöntemde eşanlamlı kelimelere birincil ve ikincil değerler atanmaktadır.
- Sonra bu değerler “1” ve “0” olarak binary’e dönüştürülür.
  - Örneğin “*big*” kelimesi birincil, “*large*” kelimesi de ikincil olarak işaretlenmiş olsun.
  - Birincil “1”, ikincil de “0” olarak binary’e çevrilir.

Görüntü Steganografi

Bilgilerin görüntü dosyaları içerisine saklanmasının çeşitli yöntemleri vardır. Bunlar:

1. En önemsiz bite ekleme
2. Maskeleme ve filtreleme
3. Algoritmalar ve dönüşümler

1- En Önemsiz Bite Ekleme (Least Significant Bit Insertion)

- En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulaması basit bir yöntemdir.
- Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır.
- 0-255 arası 1 byte ile temsil edilen gri-seviye (gray-scale) görüntüler vardır.
- Renkli dijital görüntüler 24 bit yada 8 bit olabilir.

24 bit görüntüler

- 24 bitlik bir görüntü bir pixel başına 3 byte kullanmaktadır.
- Her pixel için renk üç ana renkten elde edilir.
  - Kırmızı (red), Yeşil (green), Mavi (blue)
- Her byte'ta son biti değiştirmek suretiyle her pixel'de 3 bitlik bilgi saklayabiliriz.
- Yani 24 bitlik 1024x768 resim, bilgi saklamak için kullanılabilir 2.359.296 bit (294.912 byte)'e sahiptir.
- Eğer gizlemek istediğimiz mesajı resmin içine gömmeden önce sıkıştırırsak çok daha fazla sayıda bilgiyi gizleyebiliriz.

8 bit görüntüler

- 8 bitlik görüntüler pixel başına 1 byte kullanmaktadırlar.
- 8 bitlik görüntüler renk sınırlaması yüzünden pek iyi bir sonuç vermezler.
- Saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde dikkatlice seçilmelidir.
- Orijinal görüntüde son bite ekleme işlemi yapıldığında, renk girişi göstergeleri değişmektedir.
- 8 bitlik görüntülerde 4 basit renk kullanılmaktadır. Bunlar; beyaz, kırmızı, mavi ve yeşildir.
  - Bu renklerin renk paletinde karşılık gelen girişleri ise sırasıyla şöyledir:
    - 0 (00), 1 (01), 2 (10), 3 (11)

Gri-seviye görüntüler

- Bununla 0 (siyah) ile 255 (beyaz) arasında tam sayılar elde edilebilir. Bu sayılar arasındaki değerler gri'dir ve bundan dolayı bir resime ait tam sayı "gri ton seviye" (gray level) olarak isimlendirilir.
- İkili sayı sistemine göre 10110111 sayısını ele alalım. Bu sayı onluk düzende 183 sayısının karşılığıdır.
- Sondaki bit'in 1 veya 0 olması bu değeri çok fazla değiştirmeyecektir.
- Sondaki bit değerimiz eğer 0 olsaydı bu değer 182 olacak ve renk üzerinde gözle görülecekbüyük bir değişikliğe neden olmayacaktır.

2- Maskeleme ve Filtreleme (Masking and Filtering)

- Maskeleme ve filtreleme teknikleri genellikle 24 bit ve gri-seviye görüntüler üzerinde işaretleme (marking) ve filigran yapılarak uygulanmaktadır.
- İşaretleme yada filigran tekniklerinin görüntülere sıkça uygulanması nedeniyle, görüntünün değişmesi korkusu olmadan uygulanabilmektedir.
- Teknik olarak filigran bir steganografik biçim değildir.

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

- Son bite ekleme yöntemi bilgi gizlemek için oldukça kolay ve hızlı bir yöntemdir, fakat görüntüye uygulanan işlemler yada kayıplı sıkıştırmalar sonucunda bilgi zarar görebilmektedir.
- Yüksek kalitedeki resimlerin sıkıştırılarak örneğin jpeg formatı kullanılarak internet üzerinden gönderilmesi daha uygundur. Bunun için gizlenen bilginin kaybolmaması ve görüntünün sıkıştırılmasını sağlayan bazı yöntemler ve steganografik araçlar ortaya çıkarılmıştır.

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

Hem sıkıştırma hemde bilgi gizleme işlemlerini yapan

- Jpeg- jsteg
- Stego-Dos
- Picture-Mark
- SureSign
- S-Tools

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

Orjinal resim

Stego-Dos kullanılarak içine veri gömülmüş resim

Ses Steganografi

İnsan işitme sistemi (Human auditory system-HAS) aralığı yüzünden, ses sinyalleri içerisine bilgi gizleme oldukça uğraş gerektiren bir konudur.

HAS 1/1.000'den daha büyük frekans aralığını farkedebilir. Aynı zamanda HAS nereden geldiği belli olmayan gürültülere de oldukça duyarlıdır.

Ses Steganografi

Ses sinyalleri üzerinde uğraşırken ses dosyalarının hangi karakteristiklere sahip olduklarını bilmemiz gerekmektedir. İki ana özelliğe sahiptirler:

Basit niceleme (quantisation) metodu: Yüksek kaliteli dijital seslerin 16-bit doğrusal niceleme ile ifadesinde en çok kullanılan yöntemdir. WAV(Windows Audio-Visual) ve AIIF(Audio Interchange File Format). Bazı sinyal bozulmaları bu formatta ortaya çıkabilir.

Geçici seçme oranı: Ses için en çok kullanılan oranlar 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz ve 44.1 kHz ‘dir. Bu değer frekans aralığının kullanılabilecek en üst seviyesidir.